Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:33:21 UTC

Tool: Emissary

Names	Emissary
Category	Malware
Type	Backdoor
Description	(Palo Alto) This Trojan is related to the Elise backdoor described in the Operation Lotus Blossom report. Both Emissary and Elise are part of a malware group referred to as “LStudio”, which is based on the following debug strings found in Emissary and Elise samples. There is code overlap between Emissary and Elise, specifically in the use of a common function to log debug messages to a file and a custom algorithm to decrypt the configuration file. The custom algorithm used by Emissary and Elise to decrypt their configurations use the “srand” function to set a seed value for the “rand” function, which the algorithm uses to generate a key. While the “rand” function is meant to generate random numbers, the malware author uses the “srand” function to seed the “rand” function with a static value. The static seed value causes the “rand” function to create the same values each time it is called and results in a static key to decrypt the configuration. The seed value is where the Emissary and Elise differ in their use of this algorithm, as Emissary uses a seed value of 1024 and Elise uses the seed value of 2012. While these two Trojans share code, we consider Emissary and Elise separate tools since their configuration structure, command handler and C2 communications channel differ. The Emissary Trojan delivered in this attack contains the components listed in Table 1. At a high level, Emissary has an initial loader DLL that extracts a configuration file and a second DLL containing Emissary’s functional code that it injects into Internet Explorer.
Information	<https://unit42.paloaltonetworks.com/attack-on-french-diplomat-linked-to-operation-lotus-blossom/> <https://unit42.paloaltonetworks.com/emissary-trojan-changelog-did-operation-lotus-blossom-cause-it-to-evolve/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0082/>

Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.emissary>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool Emissary

Changed	Name	Country	Observed	
APT groups				
	Lotus Blossom, Spring Dragon, Thrip		2012-Aug 2024	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ff940eeb-a58a-41f6-93ca-8f61eb3abe46